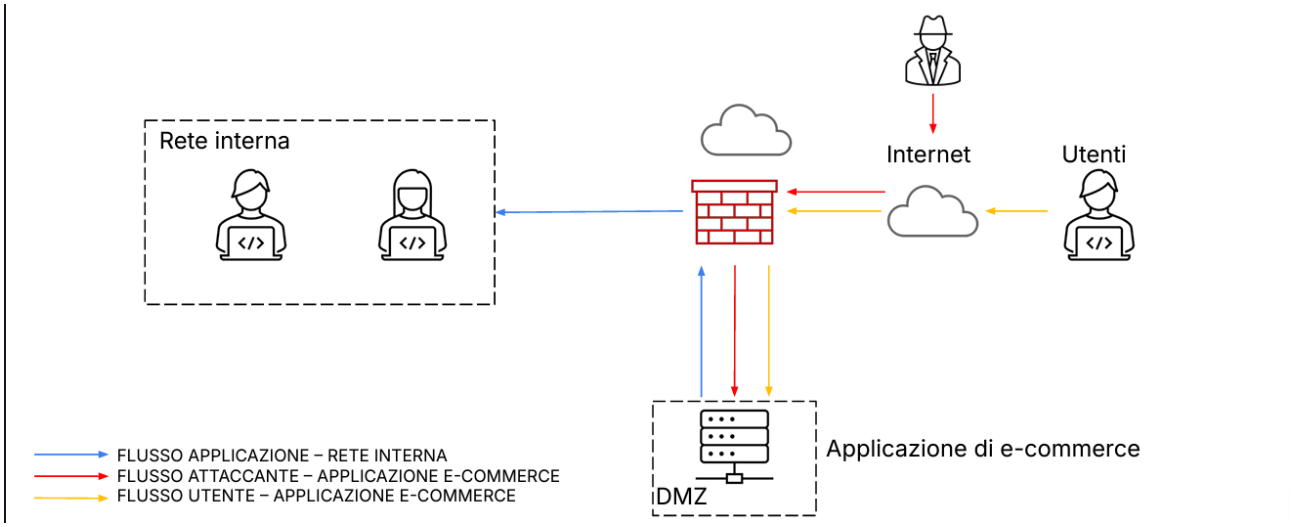
W20D4

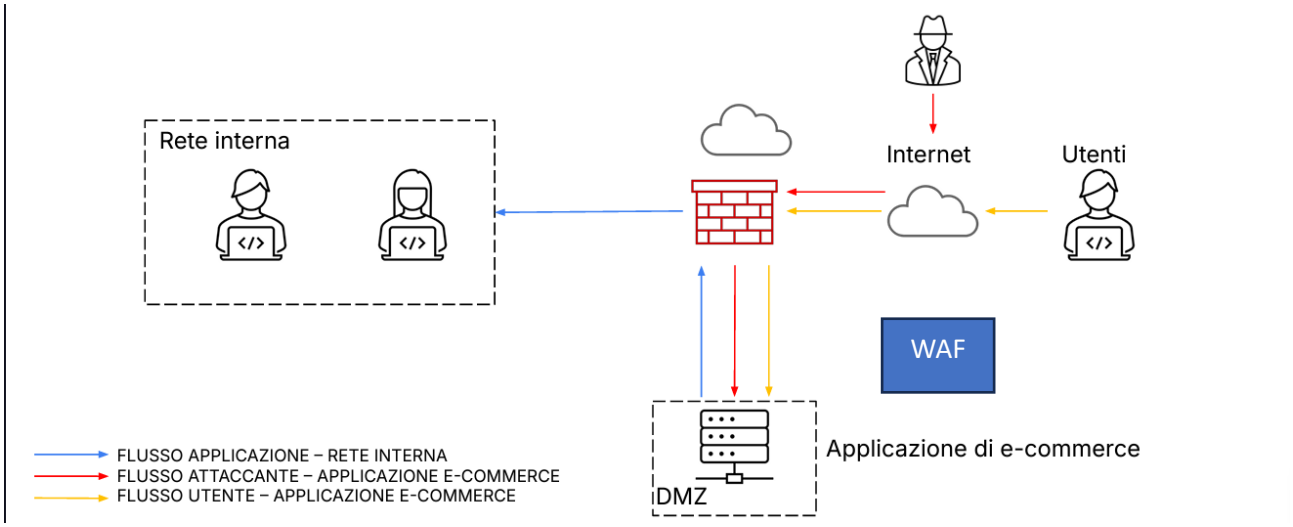


1. Azioni preventive per SQLi e XSS

Per proteggere l'applicazione da attacchi SQL injection (SQLi) e cross-site scripting (XSS), ecco alcune azioni preventive che si potrebbero implementare:

- **Sanitizzazione dei dati**: Implementare la sanitizzazione degli input per rimuovere o convertire caratteri dannosi. Gli input dell'utente devono essere verificati prima di essere inviati al database o eseguiti nel browser.
- **Parametrizzazione delle query SQL**: Utilizzare query SQL parametrizzate per impedire l'iniezione di codice malevolo. Le query parametrizzate, sono query che per la loro esecuzione, richiedono l'inserimento di, appunto, parametri, (si possono pensare anche come variabili). Solitamente la si usa nei linguaggi di programmazione per prevenire attacchi SQL injection.
- **Validazione lato server e lato client**: Aggiungere convalida a livello di server per garantire che tutti gli input siano corretti e conformi ai parametri attesi.
- **Firewall Web Application (WAF)**: Aggiungere un firewall per applicazioni web in grado di analizzare e bloccare traffico sospetto, riducendo la probabilità di attacchi SQLi o XSS.
- **Content Security Policy (CSP)**: Implementare politiche di sicurezza dei contenuti per mitigare gli attacchi XSS. Il CSP specifica quali risorse sono autorizzate a caricare i contenuti.

Modifica della figura: La figura può essere aggiornata aggiungendo un firewall WAF tra la DMZ e gli utenti esterni (internet). Inoltre, si potrebbero aggiungere icone che indicano la presenza di una validazione a livello applicativo e una query parametrizzata all'interno dell'applicazione e-commerce.



2. Impatti sul business durante un attacco DDoS

Se l'applicazione web subisce un attacco DDoS e rimane non raggiungibile per **10 minuti**, l'impatto economico può essere calcolato come segue:

- Ogni minuto gli utenti spendono 1.500 €.
- L'indisponibilità del sito dura 10 minuti.

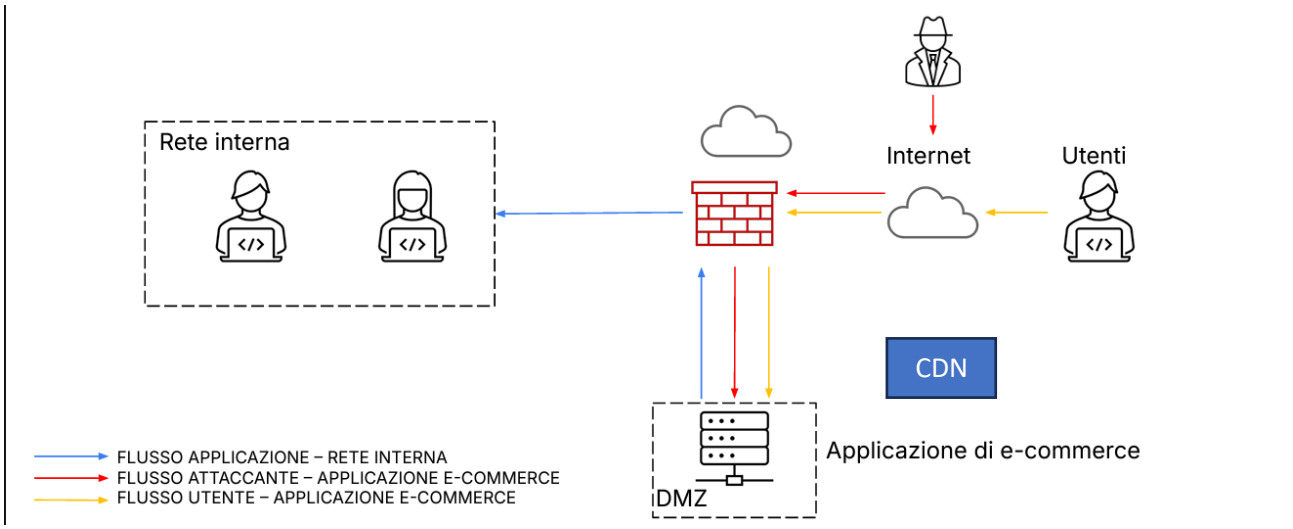
Impatto economico = 1.500 € x 10 minuti = **15.000 € di perdita**.

Azioni preventive per mitigare un attacco DDoS:

- **CDN e servizi di bilanciamento del carico**: Distribuire il traffico su più server e utilizzare una Content Delivery Network (CDN) per ridurre il rischio di sovraccarico. Grazie alla CDN si riducono notevolmente i tempi di caricamento di una pagina perché quando un contenuto viene richiesto, a rispondere è il server più vicino geograficamente e ciò si ripercuote positivamente sulle prestazioni del sito. Vi sono numerosi vantaggi che derivano dall'uso di una CDN. Oltre al miglioramento delle prestazioni, queste reti offrono anche una maggiore protezione contro gli attacchi DDoS, ma non solo. Consentono anche di attivare un meccanismo con cui gli elementi statici come pagine HTML, immagini, fogli di stile, ecc. vengono salvati temporaneamente nella cache di un server di replica, il che migliora la velocità di una pagina. I contenuti quindi non vanno richiamati tutte le volte da un server web, ma saranno già immagazzinati nel server che impiegherà quindi meno tempo per la riproduzione. Allo stesso tempo, viene garantita così la disponibilità dei servizi.
- **Firewall per applicazioni distribuite**: Implementare un firewall a livello di rete e di applicazione per mitigare gli attacchi DDoS.

- **Monitoraggio del traffico**: Implementare un sistema di monitoraggio per rilevare e bloccare traffico anomalo.

Modifica della figura: Aggiungere un'icona che rappresenta un servizio di bilanciamento del carico e una CDN esterna, tra la DMZ e internet.



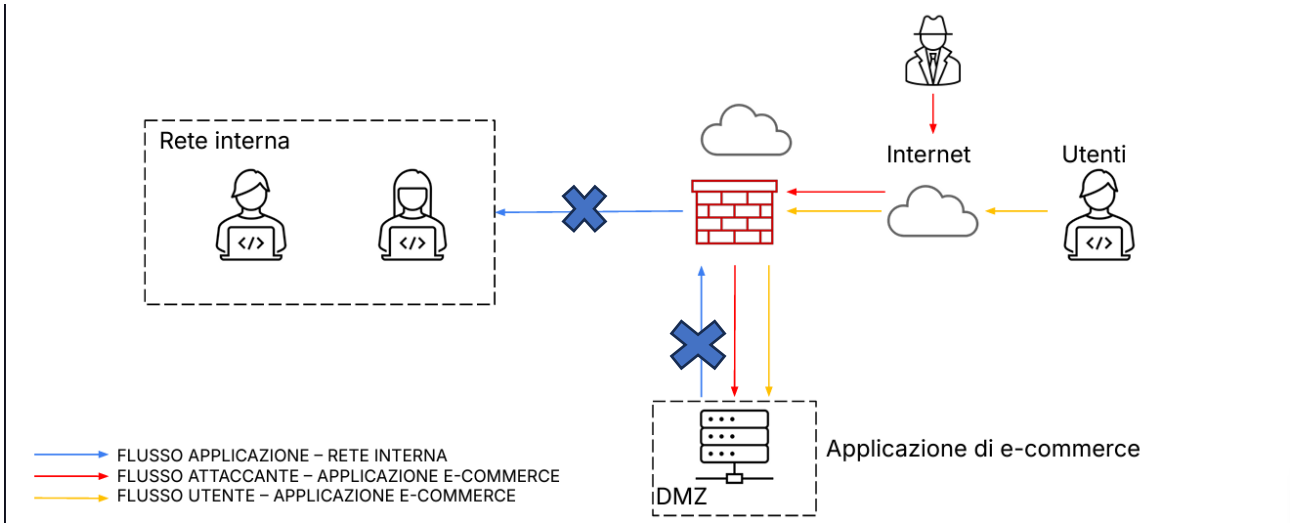
3. Response: Malware nell'applicazione Web

Quando si scopre che l'applicazione web è stata infettata da un malware, la priorità è impedire che il malware si propaghi all'interno della rete interna.

Azioni di contenimento:

- **Isolamento della DMZ**: Limitare immediatamente tutte le comunicazioni tra la DMZ e la rete interna.
- **Segmentazione della rete**: Assicurarsi che la DMZ sia completamente segmentata dalla rete interna, limitando i danni.
- **Controlli del traffico**: Implementare regole di firewall che consentono solo il traffico strettamente necessario.

Modifica della figura: Aggiornare la figura mostrando il traffico tra la DMZ e la rete interna bloccato temporaneamente.



4. Soluzione completa

Per combinare le soluzioni preventive e di risposta:

- **Prevenzione SQLi/XSS**: Aggiungere il firewall WAF e sanitizzazione dei dati.
- **Response Malware**: Segregare la DMZ dalla rete interna e bloccare il traffico, come mostrato nel punto 3.

La nuova architettura mostrerebbe:

- **Firewall WAF**: Tra internet e la DMZ.
- **CDN e bilanciamento del carico**: Per mitigare i DDoS.
- **Isolamento temporaneo**: Della DMZ dalla rete interna in caso di compromissione.

5. Modifica più aggressiva dell'infrastruttura

Una modifica aggressiva potrebbe includere:

- **Implementazione di un servizio cloud-based**: Distribuire l'applicazione in un ambiente cloud scalabile per mitigare gli impatti di attacchi DDoS.
- **Isolamento totale delle reti interne sensibili**: Aggiungere ulteriori livelli di segmentazione per proteggere risorse critiche.
- **Automazione della risposta agli attacchi**: Utilizzare strumenti di Security Information and Event Management (SIEM) per automatizzare la risposta agli attacchi e attivare la segmentazione delle reti automaticamente in caso di infezione.
- Si può anche includere un sistema di **Intrusion Detection/Prevention System (IDS/IPS)** tra la **DMZ** e la **rete interna** per prevenire ulteriori minacce.